United States Senate
WASHINGTON, DC 20510

November 12, 2019

The Honorable Mark T. Esper
Secretary of Defense
U.S. Department of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

Dear Secretary Esper:

We write to inquire about the current efforts by the Department of Defense (DoD) to educate servicemembers and DoD civilian employees about online disinformation campaigns and other malign influence operations by Russian, Chinese, and other foreign entities and individuals. While DoD is currently authorized to provide training to all servicemembers and DoD civilian employees about measures by the Russian government and its proxies to influence and recruit servicemembers as part of its malign influence campaign,[1] the Department is not formally required to provide this training. Identifying these measures can improve servicemembers' cyber security and their ability to detect and avoid falling prey to scams and other forms of manipulation. Accordingly, we are interested in understanding how DoD is using available resources effectively and appropriately to protect servicemembers from foreign malign influence operations that could undermine our democracy.

A recent investigative report by the Vietnam Veterans of America (VVA) determined that "known Russian propaganda and similar politically divisive content that targets servicemembers and veterans is being spread by admin[istrators] from at least 30 foreign countries," and that "[t]hese foreign admin[istrators] have created individual social media accounts that purport to belong to American veterans working at reputable veterans organizations."[2] The VVA investigation revealed that foreign administrators from multiple countries have impersonated servicemembers on social media, including in 2018, the professional networking platform "LinkedIn was singled out as a platform exploited by China through the use of impostor accounts meant to blend in with those of MilVets [(i.e., servicemembers and veterans)] and intelligence professionals."[3] Malicious foreign actors, according to the VVA report, also created "websites meant to mislead as well as mine data from and implant malicious software into the computer systems" of servicemembers and veterans.[4] A recent bipartisan report by the Senate Intelligence Committee on Russia's use of social media to interfere in the 2016 U.S. election observed that

---

[1] National Defense Authorization Act for Fiscal Year 2018, Public Law 115-91.
[2] Vietnam Veterans of America, "An Investigation Into Foreign Entities Who Are Targeting Servicemembers and Veterans Online," Kristofer Goldsmith, September 17, 2019, https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf; The New Republic, "Russian Trolls Love Targeting U.S. Veterans," Jasper Craven, September 18, 2019, https://newrepublic.com/article/155105/russian-trolls-love-targeting-us-veterans.
[3] *Id.*
[4] *Id.*

LinkedIn "and its users are a significant target for foreign intelligence services [...] LinkedIn users submit, and make publicly accessible, significant personal and professional data in the pursuit of networking opportunities and to attract potential employers. This renders the platform a valuable source of information on an array of sensitive intelligence targets—including the identities of government employees, active duty military personnel, cleared defense contractors, and others."[5] The malicious targeting of servicemembers is widespread, aggressive, and continuous.

We recognize that the Department understands, and is working to deter, the threats posed by online disinformation and other malign influence campaigns by foreign adversaries and other malicious actors. In recent public remarks, you observed, "The Department of Defense has an important role in defending the American people from this misinformation, particularly as it pertains to preserving the integrity of our democratic elections."[6] The Fiscal Year 2018 National Defense Authorization Act (NDAA) includes the following provision: "In addition to any currently mandated training, the Secretary of Defense may furnish annual training to all members of the Armed Forces and all civilian employees of the Department of Defense, regarding attempts by the Russian Federation and its proxies and agents to influence and recruit members of the Armed Forces as part of its influence campaign."[7]

The VVA report's recommendations for addressing online disinformation targeting servicemembers include directing DoD to "create a working group to study the security risks inherent in the use of common personal electronic devices and apps at home and abroad by servicemembers," and to "direct commanders to include personal cybersecurity training and regular cyber-hygiene checks for all servicemembers."[8] We believe that DoD should implement these recommendations, consistent with existing efforts to counter foreign malign influence operations.

Given that malicious foreign actors are targeting servicemembers using disinformation through social media platforms and other online tools and that countering foreign interference in American elections is critical to protecting the integrity of our democracy, we request that you provide unclassified responses to the following questions by December 6, 2019:

1. Is the Department implementing or has it implemented the VVA recommendations that DoD "create a working group to study the security risks inherent in the use of common personal electronic devices and apps at home and abroad by servicemembers," and that it "direct commanders to include personal cybersecurity training and regular cyber-hygiene checks for all servicemembers"?

---

[5] Senate Committee on Intelligence, "Report on Russian Active Measures Campaigns and Interference in the 2016 Election, Volume 2: Russia's Use of Social Media with Additional Views," October 8, 2019, https://www.warner.senate.gov/public/_cache/files/0/d/0dc0e6fe-4d52-49b0-9e92-a15224a74a29/C2ABC2CD38BA3C5207D7FA5352D53EC2.report-volume2.pdf.

[6] U.S. Department of Defense, "Esper Describes DOD's Increased Cyber Offensive Strategy," September 20, 2019, https://www.defense.gov/explore/story/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/.

[7] National Defense Authorization Act for Fiscal Year 2018, Public Law 115-91.

[8] Vietnam Veterans of America, "An Investigation Into Foreign Entities Who Are Targeting Servicemembers and Veterans Online," Kristofer Goldsmith, September 17, 2019, https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf.

2. How does DoD educate servicemembers about online disinformation and other malign influence campaigns by foreign governments, entities, or individuals? Is there a designated DoD official who is tasked with helping servicemembers understand these malicious activities?
3. How does DoD work with other federal agencies to educate servicemembers about online disinformation and other malign influence campaigns by foreign governments, entities, or individuals?
4. How does DoD work with social media platforms, such as Facebook and Twitter, to educate servicemembers about disinformation campaigns on these platforms?
5. What training at DoD is currently required for servicemembers to help them identify and resist attempts by foreign governments and their proxies and agents to influence and recruit members of the Armed Forces? What optional training is offered?

Thank you for your attention to this matter.

Sincerely,

Elizabeth Warren
United States Senator

Sherrod Brown
United States Senator

Mark R. Warner
United States Senator

Tammy Duckworth
United States Senator

Richard Blumenthal
United States Senator

Edward J. Markey
United States Senator

Chris Van Hollen
United States Senator

Richard J. Durbin
United States Senator

Catherine Cortez Masto
United States Senator

Tom Udall
United States Senator

Bernard Sanders
United States Senator

Tammy Baldwin
United States Senator

Doug Jones
United States Senator

Ron Wyden
United States Senator

Robert Menendez
United States Senator

Mazie K. Hirono
United States Senator

Kirsten Gillibrand
United States Senator

Jack Reed
United States Senator

Amy Klobuchar
United States Senator

Kamala D. Harris
United States Senator